AOIT Computer Networking

Lesson 13

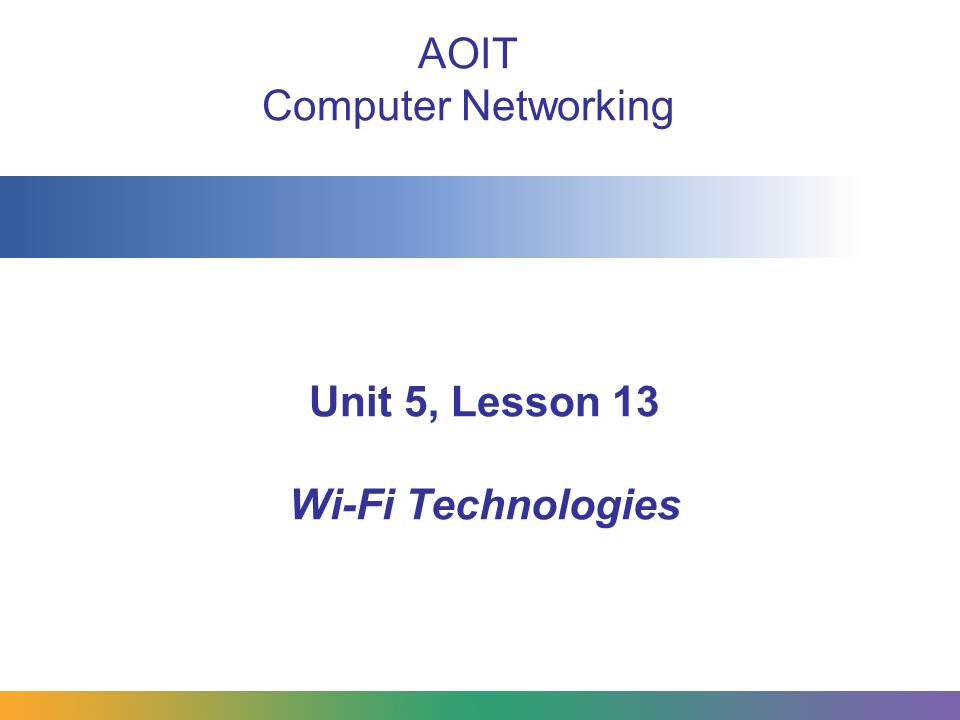
Advanced Topics in Computer Networking

Student Resources

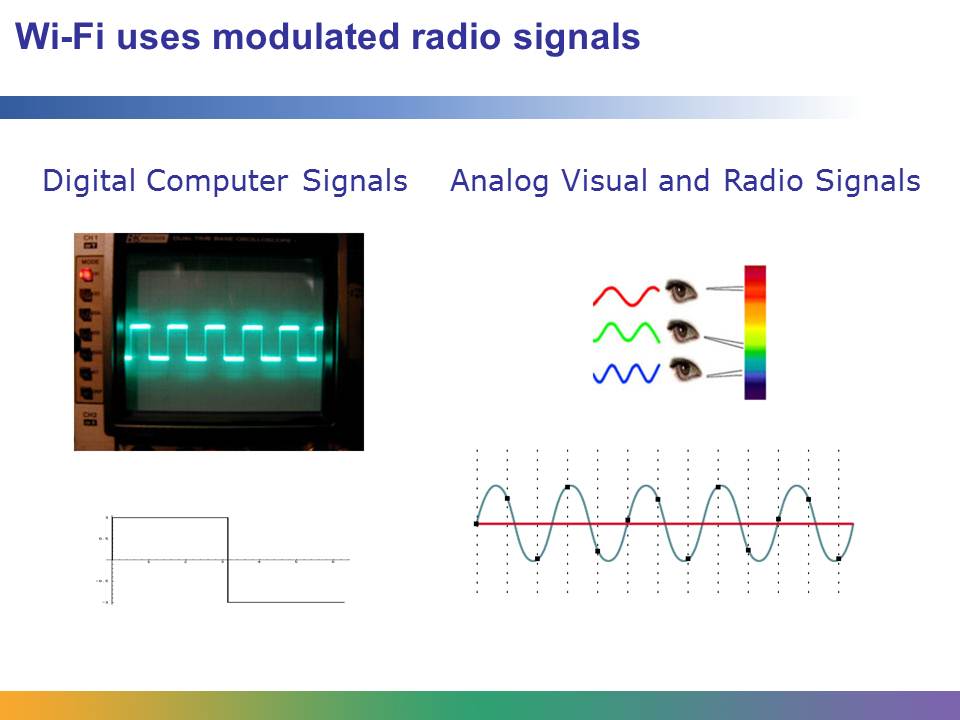
|  |  |
| --- | --- |
| Resource | Description |
| Student Resource 13.1 | Reading: Wi-Fi Technologies |
| Student Resource 13.2 | Reading: Wi-Fi and Other Wireless Networking Technologies |
| Student Resource 13.3 | Reading: Wireless Security Risks |
| Student Resource 13.4 | Worksheet: Introduction to Voice over Internet Protocol (VoIP) |
| Student Resource 13.5 | Reading: Introduction to Voice over Internet Protocol (VoIP) |

Student Resource 13.1

Reading: Wi-Fi Technologies

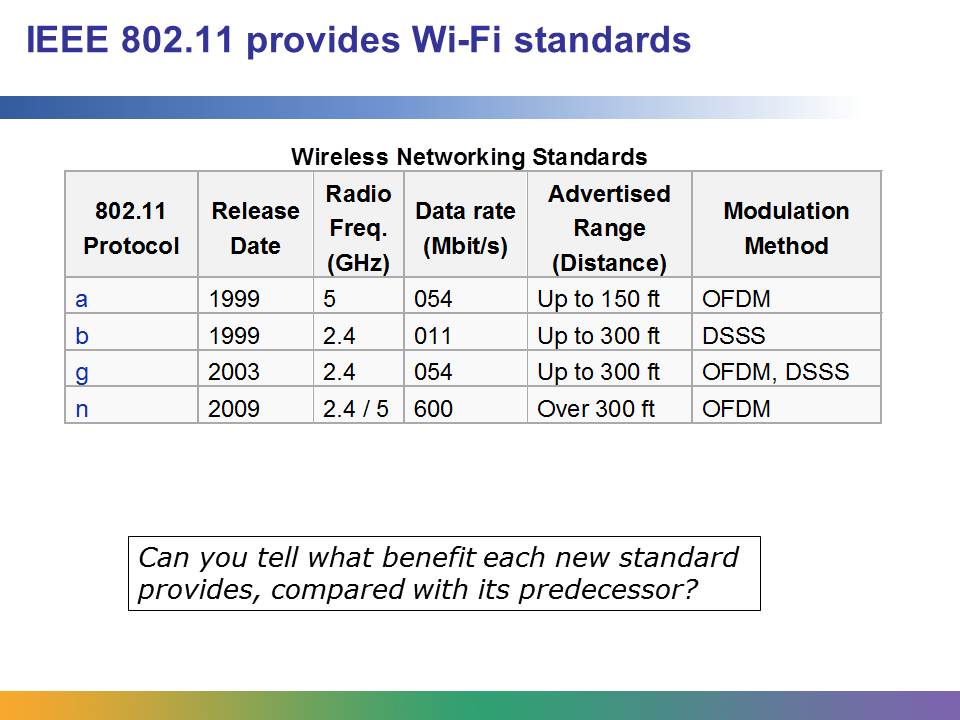


This presentation introduces the different wireless standards for computer networking—802.11a, 802.11b, 802.11g, and 802.11n—and the differences between them.



Earlier in this course you learned that computers use electric signals to communicate. These electric signals are depicted as a square wave because they have two states: on and off. In contrast, radios use analog signals with a continuous wave.

On the physical layer, wireless networks also use modulated radio signals, but they are transmitted through the air instead of via wires and cabling. WiFi is simply a radio used in computer devices.

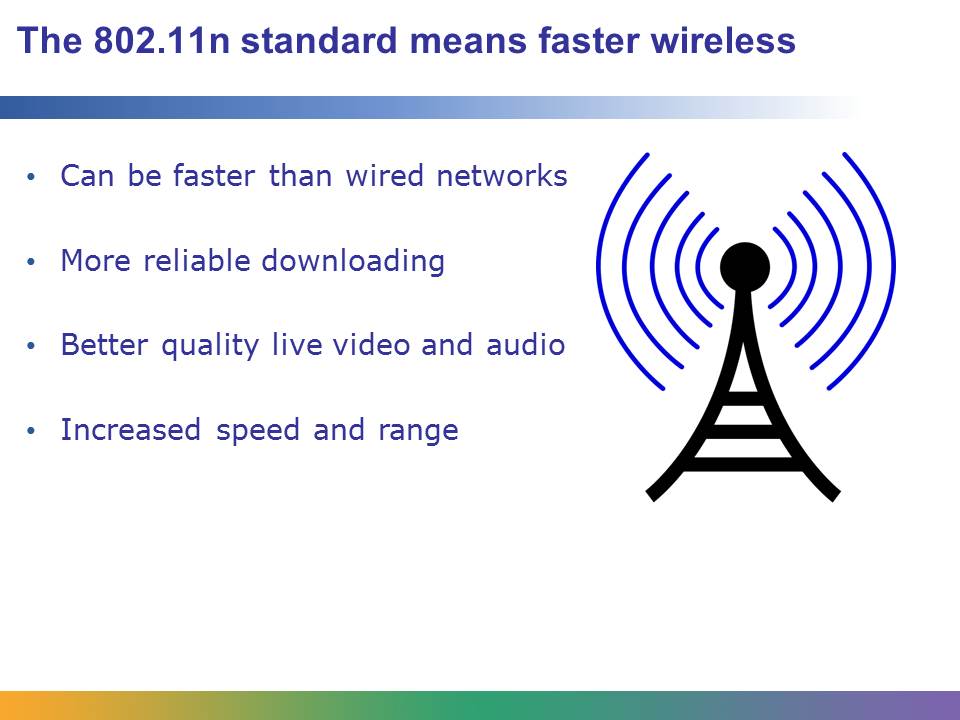


Wireless didn’t become a reliable method for computer networking until the late 1990s, when the 802.11 standard for wireless networking was developed by the IEEE. Standard 802.11a, realistically, has an indoor range limitation of about 60 feet. This is why 802.11b (300 ft.) became popular and replaced 802.11a.

The most important parts of IEEE 802.11 are the standards for communication that we use today: a, b, g, and n. Other standards in the 802.11 group, such as 802.11c through 802.11f, add amendments or changes to improve some aspects of how the service works.

The wireless networking standards use two unlicensed frequencies, at 5 GHz or 2.4 GHz, to communicate. Using 2.4 GHz, for the 802.11b and g standards, can cause interference from appliances like microwave ovens and cordless telephones that use the same frequency. The b and g standards can’t communicate with 802.11a devices, because they operate at a different frequency. The 802.11n standard uses both frequencies, so it’s compatible with all previous standards.

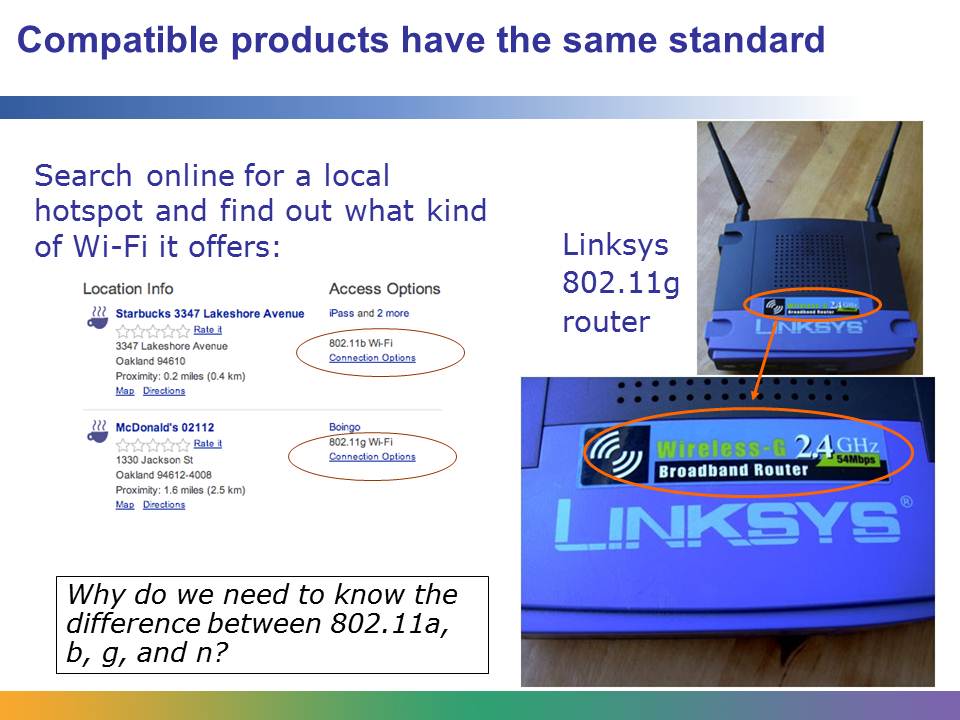
The network doesn’t always perform at the speed and range advertised. This is because walls, trees, and appliances can cause interference with the signal that slows the network and prevents the signal from traveling as far. Other wireless devices broadcasting in the same area can cause interference, too. And when the computer is farther from the wireless router, the network speed slows considerably.



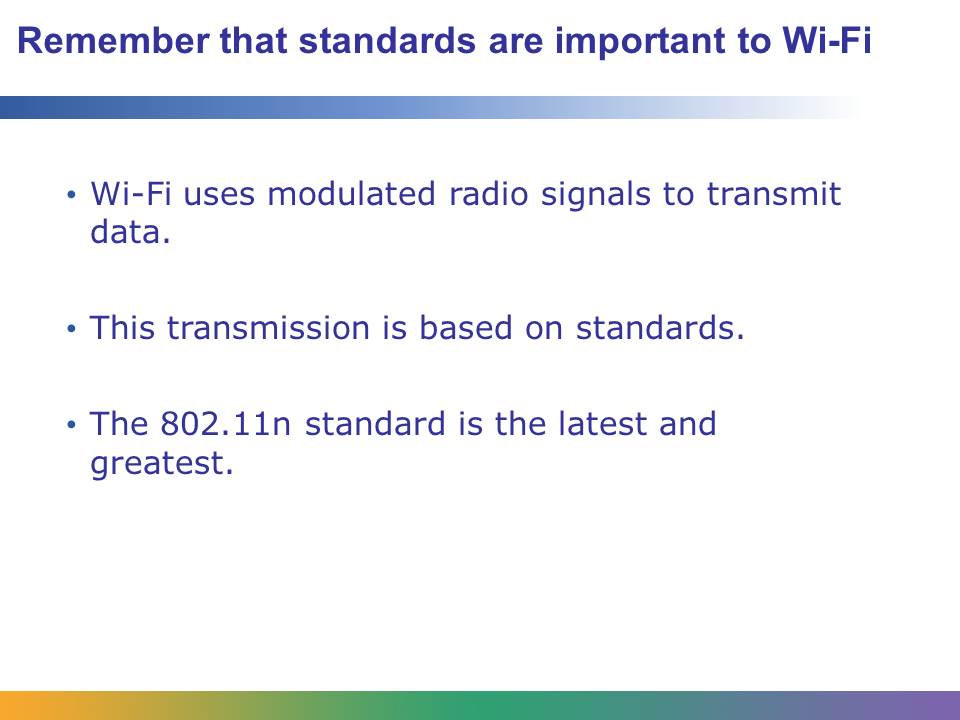
The emergence of the 802.11n standard in 2009 increased the maximum data rate from 54 Mbit/s to 600 Mbit/s by using multiple antennas at both the transmitter and receiver so there are four streams of data instead of one. This is called MIMO, or *multiple input, multiple output.* The antennas at each end of the communications circuit are combined to minimize errors and optimize data speed. This helps eliminate shadow signals from buildings and bad reception. 802.11n devices are much faster and more reliable and work across greater distances than devices using earlier standards.

With the 802.11n standard, residences and businesses are relying more and more on wireless networks. Many vendors developed consumer-grade products like wireless routers and networking cards based on the 802.11n standard even before the rules for it were finalized, hoping they would be able to upgrade the early products to the final standard.

Tower image: http://commons.wikimedia.org/wiki/File:Wireless\_tower.svg. Permission is granted to copy, distribute, and/or modify this image under the terms of the GNU Free Documentation License.



When you are looking for any product for wireless networking—whether it’s a wireless router for your home, a computer with a wireless networking card, or a wireless hotspot in your area—you’ll want to find out what standard is offered. For example, if you have a computer with an old wireless adapter using 802.11a, it won’t be compatible with a hotspot that offers only 802.11b or 802.11g. If you’re getting a new wireless router for your home, you’ll need to consider whether to get an older standard like 802.11b or 802.11g, or whether to get the latest standard, 802.11n.



Wi-Fi for computer networking uses modulated radio signals to transmit data across distances.

Different wireless standards—802.11a, 802.11b, 802.11g, and 802.11n—use different modulation technologies and frequencies and provide different levels of service.

To use wireless technology, your network adapter must be compatible with the router.

The latest standard is 802.11n. It provides the best coverage and works with all other standards.

Student Resource 13.2

Reading:   
Wi-Fi and Other Wireless Networking Technologies

Wi-Fi

Wi-Fi refers to 802.11a, 802.11b, 802.11g, and 802.11n, the wireless standards developed for residences’ and businesses’ wireless computer networks. But the 802.11 standards are not the only type of wireless communication used for computer networks. Let’s look at some other ways that we use wireless for communications.

WiMax

A similar technology to Wi-Fi is WiMax, codified as IEEE 802.16. It is meant mostly to be used for citywide networks, or wireless networks that span a wide area outdoors in public places. It’s also ideal for rural areas where DSL and cable don’t reach easily. One network can simultaneously support hundreds of businesses and residences.

WiMax can also be used on vehicles moving between 13 to 60 miles an hour. So, public buses, trains, and other transit systems can use WiMax to allow passengers or train conductors to use a wireless connection.

Bluetooth

You may have used Bluetooth without even knowing it. Bluetooth is often used to enable computer mice, keyboards, and other peripherals to wirelessly communicate with the computer. Additionally, it is used in other devices like wireless headsets for cell phones, or in cameras that can send files to a computer or to a printer without using a USB cable to connect.

Like 802.11b and g, Bluetooth also transmits at the unlicensed spectrum frequency of 2.4 GHz. However, it uses a different modulation technique to send data. Additionally, it uses much less electric power, and the signal doesn’t travel nearly as far. So, it is good for devices that don’t need much bandwidth and are close to the device they are communicating with. Some Bluetooth devices can transmit much further than others, depending on the chip that is used.

Radio Frequency ID (RFID) Tags

Radio frequency ID tags are computer chips coded with identifying information that can be attached to boxes, clothing, or other objects. For example, a company might ship a few hundred boxes to another location, where a warehouse manager has to check that all of those boxes arrived safely. The company can attach an RFID tag to each box saying what’s in it and when it shipped, and the warehouse manager can use an RFID tag reader to check the tags on the boxes when they arrive. The tag reader is like a small handheld computer that shows the information from each tag.

The tags can be active or passive, meaning they’re not always powered up and transmitting data. The tag can be powered up by the tag reader from a distance so that it can be read. Additionally, a reader device can be networked to a computer database that looks up more information about an object, based on the identification label on the RFID tag. Not all RFID tags work in the same way—there are over 140 different standards for RFID, because the technology has a range of uses.

Other Common Wireless Devices

In addition to computer communications equipment, you use other common wireless devices as well—from garage door openers to TV remotes. These use different technologies than the ones described in this reading. For example, garage door openers transmit radio signals at 300–400 MHz and use a digital code, set up via switches on the device, to make sure that one opener won’t open all the garage doors in the neighborhood.

TV remote controls, unlike all the technologies described so far, use a modulated infrared light signal that must be picked up by a special sensor within optical range of the control. The wireless devices that run on radio waves can usually transmit even when they are out of sight of the receiving device, such as through walls. This isn’t the case for TV remotes, because then you could change your next-door neighbor’s TV channel!

Student Resource 13.3

Reading: Wireless Security Risks

Firewalls

Firewalls are available for wireless routers as well as for client and server computers. When browsing a wireless network, make sure your computer’s firewall is enabled. If you’re using your own router instead of a hotspot, then configure the router’s firewall, too. Remember, this will prevent unwanted traffic from entering your network, because you can block network ports that you don’t need.

Wireless Encryption Security

Encryption is used to protect wireless security. Earlier Wi-Fi equipment used WEP (Wired Equivalent Privacy), which had many security weaknesses and was vulnerable to attacks. WEP has been replaced by the newer and more secure Wi-Fi Protected Access (WPA and WPA2).

WPA2 is the most recent standard. There are two versions of WPA2: WPA2-Personal, and WPA2-Enterprise. WPA2-Personal or WPA2-PSK (Pre-Shared Key), which is often used for home networks, protects unauthorized network access by using a set-up password or a pre-shared key. WPA2-Enterprise, which is used in large corporate networks, verifies network users through an enterprise authentication server.

Bluetooth Snarfing

Bluetooth devices such as smartphones often contain important information, such as an address book with phone numbers and other contact information. Since these devices also use wireless transmission, some hackers have demonstrated the ability to use another Bluetooth device to steal that information. In one instance, the hacker was able to do so from as far as a mile away. The best way to protect information is to turn off the Bluetooth in your phone or PDA when you’re not using it.

Keyloggers

One of the most dangerous risks on an unprotected wireless network, such as one at a public coffee shop, is keylogger programs. Keyloggers are a type of software that log your keystrokes and clicks. At a wireless hotspot, another person with a computer can intercept your data stream, install a keylogger, and then have the software send your keystrokes back to his computer. If you log in to bank accounts or your email, the keylogger will record your passwords, and the hacker will get access to your accounts and personal information.

Note that keylogger programs can be installed on non-wireless connections as well. Software programs installed on computers or on devices that connect between the computer and the keyboard can do keylogging.

Pharming

In a pharming attack, hackers redirect traffic from a genuine site to their own website in order to collect information such as credit card numbers from users. This happens on wireless networks but is not limited to wireless networks.

Remember that in a phishing attack, hackers will make a fake website that looks like the real one—for example, a site for a popular bank. Then, they lure users to the site through a scam email. But users can avoid this attack by finding the proper URL for the genuine website and typing it into the navigation bar at the top of the browser window.

In a pharming attack, the hackers can even send this direct traffic to their own site. They can do this by hacking the real website’s code to forward traffic. Or, they can do a “drive-by attack,” reconfiguring a wireless router. This is called “drive-by pharming” because the hackers can sit at the edge of a wireless hotspot—for example, in their car outside a coffee shop or an apartment building—and reconfigure the wireless router so that it sends all traffic to the hackers’ website.

The best way to protect against pharming is to change the default ID, network encryption, and passwords on a wireless router, so that hackers can’t reconfigure it.

Student Resource 13.4

Worksheet: Introduction to   
Voice over Internet Protocol (VoIP)

Student Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date:\_\_\_\_\_\_\_\_\_\_\_

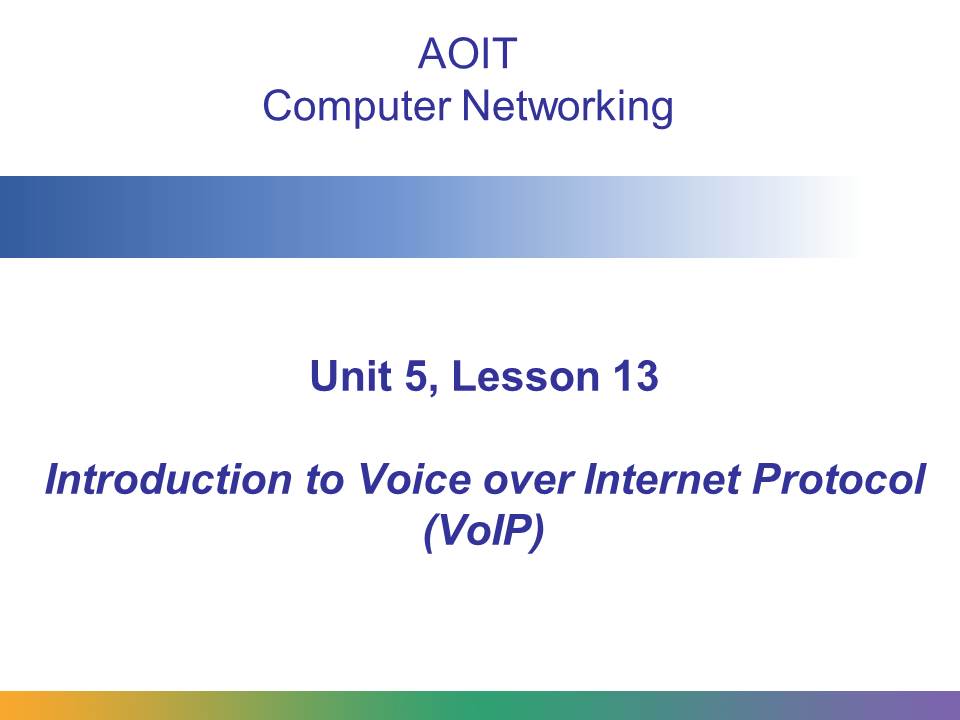
Directions: Use the following graphic organizer to record your notes about voice over Internet Protocol.

Voice over IP is…

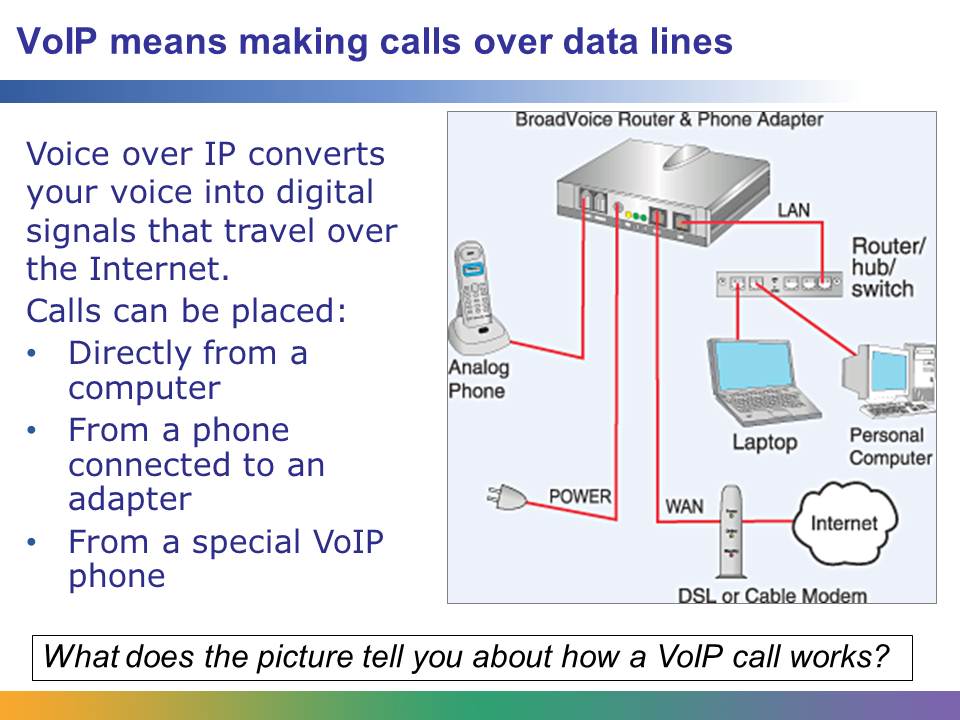
|  |  |  |
| --- | --- | --- |
| Features/Benefits | Disadvantages/Drawbacks | Other Notes |

Student Resource 13.5

Reading: Introduction to   
Voice over Internet Protocol (VoIP)



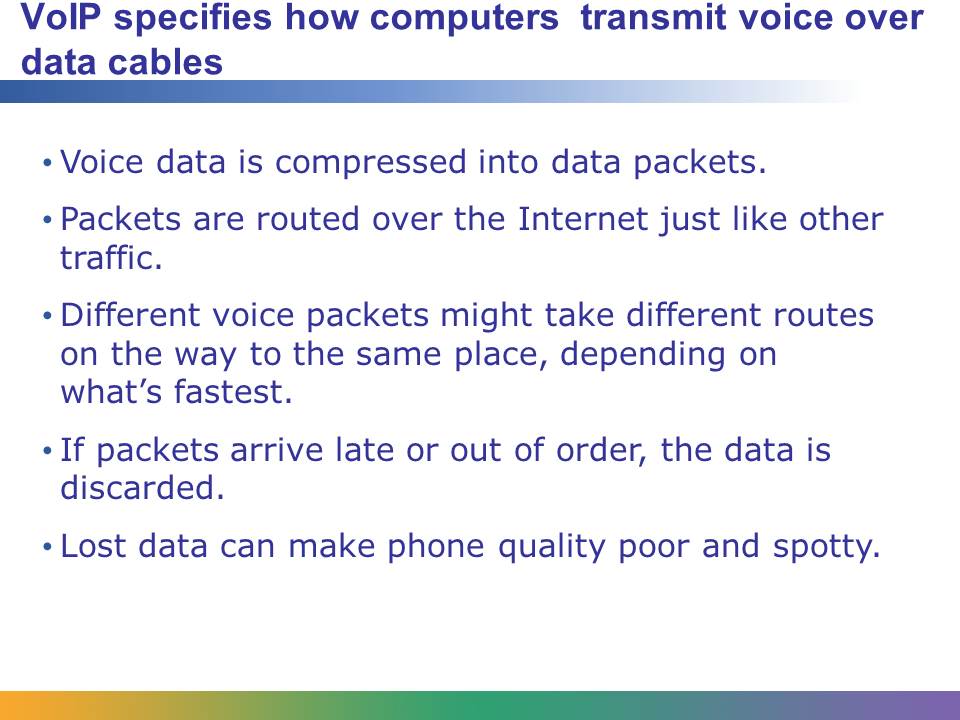
This presentation introduces students to voice over Internet Protocol: how it works and its benefits and drawbacks.



VoIP uses your Internet connection to send live voice information such as a telephone call. You need special hardware and software that can capture your voice as you speak, translate it to digital data, and send it across the digital cables.

If you are calling a regular phone number, the signal is converted to a regular telephone signal before it reaches the destination. VoIP can allow you to make a call directly from a computer, a special VoIP phone, or a traditional phone connected to a special adapter. In addition, wireless "hot spots" in locations such as airports, parks, and cafes allow you to connect to the Internet and may enable you to use VoIP service wirelessly.   
  
VoIP is available for individuals from a variety of vendors such as Skype, AOL Instant Messenger, or Gmail. However, implementing a VoIP service for a large business is quite different from using VoIP on a home computer.

Image courtesy of Wikimedia http://upload.wikimedia.org/wikipedia/commons/4/44/Voip-typical.gif



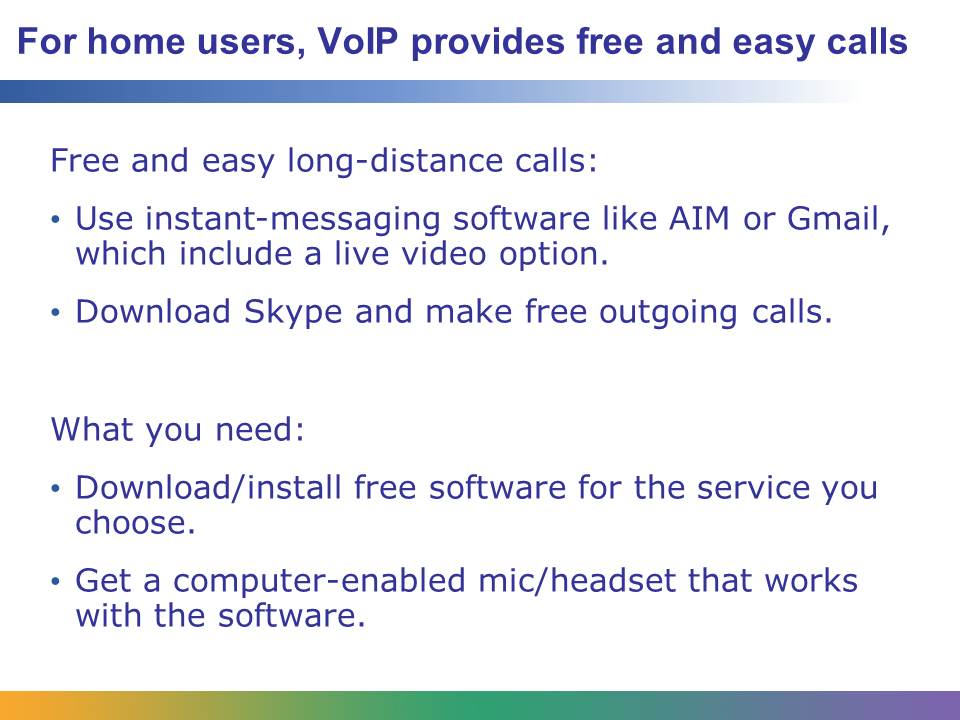
Different types of protocols for networking have different ways of sending data across the cables. Let’s review a couple of important ones:

In **Asynchronous Transfer Mode**, or ATM, a direct connection is established in order to make sure data is routed swiftly and is received in sequential order. The data cells are a certain length. (ATM uses cells rather than packets.) Historically, this meant ATM was more reliable for Internet telephone calls.

However, most of the Internet now uses **Internet Protocol**, or IP, to transmit information; this breaks data into packets and routes them across the Net from node to node. Packets might take different routes even if they’re headed for the same destination. Upon arrival, they are reassembled in sequential order.

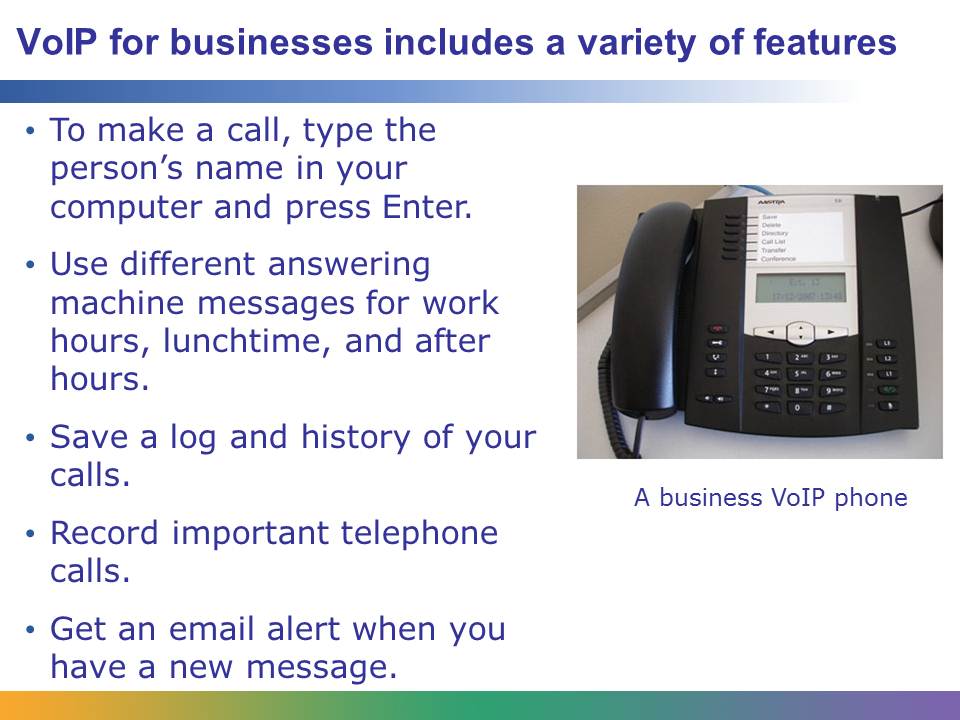
**Voice over IP**, or VoIP, makes it possible to send voice information like data packets in IP. VoIP compresses voice or sound waves into data packets, then sends them from node to node on the Internet. The packets are labeled with headers that explain the destination of the packet and the packet sequence, then each packet is sent separately depending on the route that’s quickest at the moment.

VoIP presents some challenges, because on a telephone call, everything needs to happen swiftly and in the right order. So, if Packet A is late but Packets B, C, and D arrive on time, Packet A is dropped. The others are uncompressed and translated to sound waves so that the receiver can hear what’s being said. If lots of packets are lost, the voice quality you hear is bad.



Home users and small-business consumers can easily use free VoIP services to make calls over the Internet. Instant-messaging software like AIM and Gmail offer an audio capability so that users can speak with each other rather than typing, and Skype allows free outgoing calls.

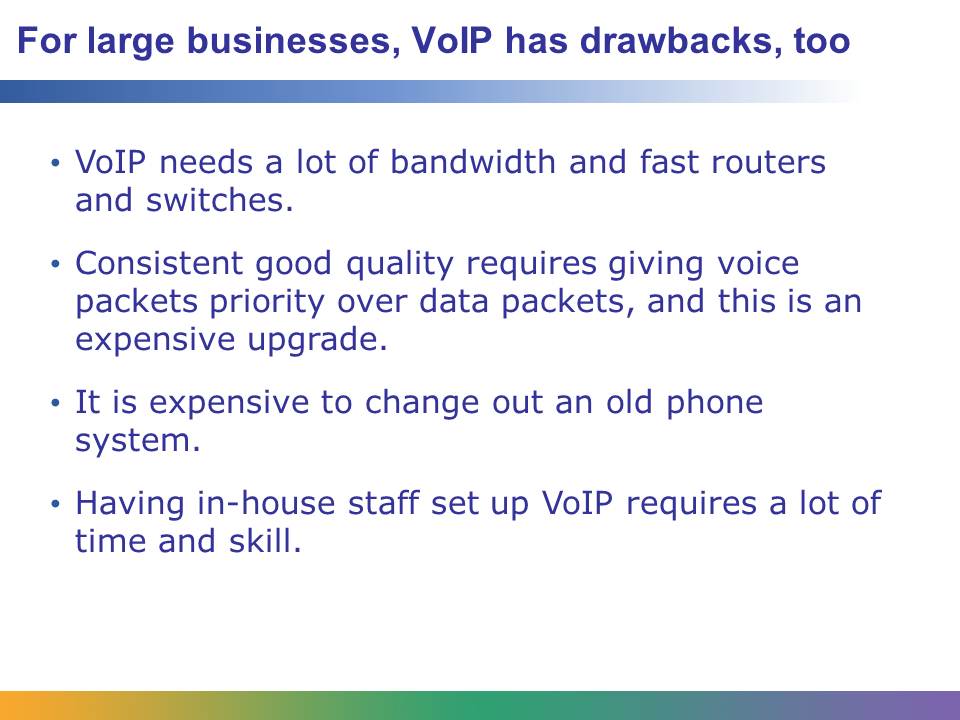
For regular telephone service, consumers can also subscribe to a home VoIP service that assigns them a personal telephone number and allows them to both make and receive calls.



VoIP is more than just a different way to make phone calls. Since it uses data packets, it also integrates well with computer networks and computer systems. Some of the most useful features involve accessing information off a shared server, such as a company phone directory. Employees in a company that uses VoIP can click a box on their computer screen, type the name of another employee they want to call, and press Enter, and their phone will ring the other employee. This makes it simpler to make calls, especially in large organizations.

Some systems are more capable than others. Most will let you set different answering machine messages for different situations, and will send you email when you have new voicemail messages. Some also save a history of your calls, record phone calls for you, and do other things, too.

Many companies that have a telemarketing department or that provide a customer service hotline can benefit in other ways from the way VoIP integrates telephones and computers. For example, when you call a technical support line, an automated machine might ask for your name, the serial number of the product, and what problem you’re having, then automatically access information about your account. The system that does this is called an integrated voice response system. When the system connects you with a customer service representative, the representative’s computer might pop up a screen that tells her about your product and any previous calls you’ve made.



Although VoIP is pretty easy to use and quality is usually good for home use, installing a VoIP system in a large business requires a lot of time, money, and skill. VoIP users need phones and other network equipment, which gets expensive. The biggest concern for a large business is having enough bandwidth, but upgrades to routers and switches are also required. For large business implementations, staff need to set up the system and help users get used to the new system. If the Internet service doesn’t provide the bandwidth and speed needed, then call quality might not be good enough. To improve the call quality, companies often implement QoS (quality of service) to give voice packets a higher priority than web traffic, but this is another big upgrade.

The VoIP industry is still very young. Many vendors that offer software and services to home users or small businesses are small and may be unreliable, and have been struggling to stay in business. Companies like Cisco offer solutions for large businesses. Some businesses use open-source software to set up their own system, instead of buying software and service from a vendor. However, this can be very time-consuming to set up and requires the staff to understand very well what they are doing, so it’s not an option that all businesses can pursue. For these reasons, many companies are not yet switching over to VoIP services. But it is coming in the future. As Internet speeds get faster and as more bandwidth becomes available for less money, and as more companies grow and mature in the VoIP space, it will become easier for businesses to switch to VoIP telephone systems.



VoIP has lots of advantages over regular phone service, even though there are still a few kinks in the system. Most of these disadvantages are being overcome as technology changes and innovations continue. It is possible that VoIP will eventually replace traditional phone service. VoIP has started to receive widespread consumer acceptance, and there is a tremendous amount of work being done to increase the reliability and usefulness of VoIP.